Finite Fields and Their Applications **5,** 1–12 (1999)
Article ID ffta.1998.0229, available online at http://www.idealibrary.com on IDEAL®

# Small Complete Arcs in PG(2, $p$)

Éva Hadnagy

*Department of Mathematics, Budapest University of Economics, P.O. Box 489, 1828 Budapest, Hungary*
E-mail: vica@math.bme.hu

*Communicated by James W. P. Hirshfeld*

Received February 21, 1997; revised June 2, 1998

In this paper we construct a large family of complete arcs. Let $p$ be a prime. For any integer $k$ satisfying

$$[2.46 \cdot \ln p \cdot p^{3/4}] \le k \le \left[\frac{p+7}{3}\right] + 1,$$

there exists a complete arc of size $k$ in PG$(2, p)$. © 1999 Academic Press

## 1. INTRODUCTION

A *$k$-arc* in a projective plane of order $q$ is a set of $k$ points no three of which are collinear. The maximum number of points that a $k$-arc can have is $q + 1$, for $q$ odd, and $q + 2$, for $q$ even. A $k$-arc with this number of points is called an *oval*. A $k$-arc is called *complete* if it is not contained in a $(k + 1)$-arc.

Let $m'(2, q)$ and $n(2, q)$ denote the size of the largest and the smallest non-oval complete arc of PG$(2, q)$. Hirshfeld conjectured that a complete $k$-arc exists in PG$(2, q)$ for all values in the interval $[n(2, q), m'(2, q)]$.

If $q$ is not a square number then the best lower bound for $m'(2, q)$ is $m'(2, q) \ge (q + 2\sqrt{q})/2$. The complete arcs yielding this bound contain half the points of an elliptic cubic (see Voloch [10]). From the result of Voloch it follows that for any prime $p > 175$ and any integer $k$ satisfying

$$(\sqrt{p} - 1)^2/2 < k < (\sqrt{p} + 1)^2/2,$$



1071-5797/99 $30.00

there exists a complete $k$-arc. For sufficiently large primes $p$, Szőnyi [7] improved this interval to

$$[p/3] + 3 \leq k \leq [p/2] + 1.$$

The aim of this paper is to determine another large interval such that every $k$ from it is a size of a complete $k$-arc in PG$(2, p)$. To do this we fix an irreducible cubic curve $\mathscr{H}$ in PG$(2, p)$ and show how to construct a big family of point-sets $K$ on $\mathscr{H}$ so that $K$ is an arc and the chords of $K$ cover all points in the plane apart from those lying on $\mathscr{H}$ and on a special line. Then we obtain a complete arc by adding some extra points to $K$. Our main result is the following.

THEOREM 1.1. *Let $p$ be a prime. For any integer $k$ satisfying*

$$[2.46 \cdot \ln p \cdot p^{3/4}] \leq k \leq \left[\frac{p+7}{3}\right] + 1,$$

*there exists a complete arc of size $k$ in* PG$(2, p)$.

Theorem 1.1 together with the previous results due to Voloch and Szőnyi has the following consequence.

COROLLARY 1.2. *Let $p$ be a prime. For any integer $k$ satisfying*

$$[2.46 \cdot \ln p \cdot p^{3/4}] \leq k \leq (\sqrt{p} + 1)^2/2,$$

*there exists a complete arc of size $k$ points in* PG$(2, p)$.

Note that this interval is not empty for $p$ greater than $5 \cdot 10^8$ only.

## 2. POINTS COVERED BY CHORDS OF A CUBIC CURVE IN PG$(2, p)$

For a positive integer $c \cdot p$ $(0 < c < 1)$, let $K$ consist of the points $\{(x, x^3, 1) : x = 0, \ldots, c \cdot p\}$ on the rational cubic curve $\mathscr{H}$ of equation $YZ^2 = X^3$. We prove that $K$ is extendable to a maximal arc with at most $\lceil 1/c \rceil - 1$ points.

### 2.1. *Affine Points*

In this section we are going to show that for a sufficiently big $c$ the chords of $K$ cover all affine points not lying on $\mathscr{H}$.

Let $P \notin \mathscr{H}$ be $P(a, b, 1)$ $(a^3 \neq b)$. Then $P_1(x_1, x_1^3, 1) \in K$, $P_2(x_2, x_2^3, 1) \in K$, where $(x_1 \neq x_2)$ and $P(a, b, 1)$ are collinear if

$$a(x_1^2 + x_1x_2 + x_2^2) - x_1x_2^2 - x_1^2x_2 - b = 0.$$

We want to get a solution for this equation satisfying $0 \leq x_1 < x_2 \leq c \cdot p$ for all $P(a, b, 1)$ $(a^3 \neq b)$. We estimate the number of such solutions of

$$f(X, Y) = a(X^2 + XY + Y^2) - XY^2 - X^2Y - b = 0 \qquad \text{if } X \neq Y.$$

THEOREM 2.1. *In* PG(2, $p$), *there is a point* $(x_1, y_1)$ *with* $0 < x_1 \neq y_1 < c \cdot p$ *on the curve* $\mathscr{C}$ *with equation* $f(X, Y) = 0$ *provided that*

$$c > \frac{\sqrt{3 + (6\sqrt{p} + 9)\ln^2 p}}{\sqrt{p} - 1}.$$

*Proof.* It is straightforward to check that the cubic curve $\mathscr{C}$ with equation $f(x, y) = 0$ is absolutely irreducible. Next we estimate the number of points of $\mathscr{C}$ with coordinates over GF($p$) by using two general results on GF($q$)-rational points of algebraic curves defined over GF($q$).

THEOREM OF HASSE–WEIL. *If $f$ is an absolutely irreducible projective curve of degree $n$ defined over* GF($q$), *and $N$ denotes the number of points of $f$ that belong to* GF($q$), *then*

$$|q + 1 - N| \leq (n - 1)(n - 2)\sqrt{q}.$$

THEOREM OF SMITH. *Let $p$ be an odd prime and denote by $C$ the set of points* $\mathbf{x} = (x_1, \ldots, x_n)$ *satisfying* $0 \leq x_i < p$ $(i = 1, \ldots, n)$. *Let* $C^* = C \backslash \{(0, \ldots, 0)\}$. *We define a box* $\mathscr{B}$ *in* $C$ *as the set of all points* $\mathbf{x} \in C$, *which satisfy* $0 \leq v_i \leq x_i < v_i + h_i \leq p$ $(i = 1, \ldots, n)$. *Let* $f(\mathbf{X})$ *be a polynomial in $n$ variables* $(\mathbf{X} = (X_1, \ldots, X_n)$, $0 \leq X_i < p$, $i = 1, \ldots, n)$. *Denote by $N$ the number of* $\mathbf{X} \in \mathscr{B}$ *for which* $f(\mathbf{X}) = 0 \pmod p$. *Then*

$$N(\mathscr{B}) = \frac{|\mathscr{B}|}{|C|} N(C) + \frac{1}{|C|} \sum_{\mathbf{c} \in C^*} S_n(f, \mathbf{c}) \mathscr{E}_{\mathbf{c}}(\mathscr{B}), \tag{1}$$

(see Theorem 1 of [2]) *where*

$$\mathscr{E}_{\mathbf{c}}(\mathscr{B}) = \sum_{\mathbf{a} \in \mathscr{B}} e^{2\pi i/p \cdot (-\mathbf{a} \cdot \mathbf{c})} \quad \text{and} \quad S_n(f, \mathbf{c}) = \sum_{f(\mathbf{x}) = 0} e^{2\pi i/p \cdot (-\mathbf{c} \cdot \mathbf{x})},$$

*where the sum extends over all* $\mathbf{x}$ *satisfying* $f(\mathbf{x}) = 0$, *and* $\mathbf{c}\cdot\mathbf{x}$ *denotes the ordinary inner product of* $\mathbf{c}$ *and* $\mathbf{x}$.

To apply Smith's theorem, an upper bound for the expression on the right side of (1) is needed. For this reason we state Lemmas 1 and 2.

LEMMA 1.

$$\sum_{\mathbf{c}\in C^*} |\mathscr{E}_{\mathbf{c}}(\mathscr{B})| \le Bp^n \cdot \ln^n p. \tag{2}$$

Here $B$ is an absolute constant depending only on $n$. In our case $n = 2$. If $p > 59$, then $B = 1$ is a good choice (see section 3 of [2]).

We also need the following result:

LEMMA 2 (Lemma 1 of [6]). *Let* $f(X)$ *and* $\psi(X, Y)$ *be polynomials over* GF($p$), *where* $\deg \psi = d_1$, $\deg f = d_2$, $1 \le d_1, d_2 < p$ *and suppose* $\psi(X, Y)$ *has no linear factors. If*

$$S(f, \psi) = \sum_{\psi(x, y) = 0} e^{2\pi i/p \cdot f(x)},$$

*then*

$$|S(f, \psi)| \le (d_1^2 + 2d_1d_2 - 3d_1)p^{1/2} + d_1^2. \tag{3}$$

In our case $f(X, Y) = c_1X + c_2Y$ for some $\mathbf{c} = (c_1, c_2)$. To be able to use the previous lemma, $f$ will be transformed into a function of one variable. If $c_2 = 0$, then $f$ is already such a function. Otherwise we apply a non-singular linear transformation

$$t(X, Y) = (U, V) = (c_1X + c_2Y, X).$$

Let $f'(U)$ and $\psi'(U, V)$ be the images of $f(X, Y)$ and $\psi(X, Y)$. A linear transformation does not change the number of linear factors of $\psi$, thus $\psi'(u, v)$ has no linear factors either. Now $\deg \psi' = 3$ and $\deg f' = 1$; so

$$S_n(f', \mathbf{c}) \le (9 + 2\cdot 1\cdot 3 - 3\cdot 3)\sqrt{p} + 9 = 6\sqrt{p} + 9. \tag{4}$$

Putting (1), (2) and (4) together gives

$$N(\mathscr{B}) \ge \frac{c^2p^2}{p^2}(p + 1 - 2\sqrt{p}) - \frac{1}{p^2}(6\sqrt{p} + 9)p^2 \ln^2 p.$$

According to Bézout's theorem, the curve meets the line $y = x$ in at most three points. Hence, the curve $\mathscr{C}$ contains a point $P(x, y)$, $x \neq y$, in the required interval provided that the number on the right side is bigger than 3. Therefore

$$c^2 \cdot (p + 1 - 2\sqrt{p}) - (6\sqrt{p} + 9)\ln^2 p > 3,$$

which means that, for

$$c > \frac{\sqrt{3 + (6\sqrt{p} + 9)\ln^2 p}}{\sqrt{p} - 1}, \tag{5}$$

the chords of $K$ cover all affine points not on $\mathscr{H}$. ■

2.2. *Ideal Points*

The aim of this section is to find the ideal points covered by the chords of $K$.

THEOREM 2.2. *For $c$ as big as in Theorem 2.1, the chords of $K$ cover all ideal points other than $Y_\infty(0, 1, 0)$ and, for $p \not\equiv 1 \pmod 3$, also $X_\infty(1, 0, 0)$.*

The point $Y_\infty(0, 1, 0)$ is on $\mathscr{H}$. Let $P = P(1, m, 0)$. Then $P_1(x_1, x_1^3, 1) \in K$, $P_2(x_2, x_2^3, 1) \in K$, (where $x_1 \neq x_2$) and $P(1, m, 0)$ are collinear if

$$x_1^2 + x_1 x_2 + x_2^2 - m = 0.$$

If this quadratic form is absolutely irreducible, then it has the following consequence. Otherwise we suppose that

$$f(X, Y) = X^2 + XY + Y^2 - m$$

is reducible in the form $X^2 + XY + Y^2 - m = (X - aY + b)(X - cY + d)$. Comparison shows $b = d = m = 0$. Hence, it remains to investigate the case where the ideal point is $X_\infty$ (1, 0, 0). For $p \not\equiv 1 \pmod 3$, $X^3 = Y^3$ implies $X = Y$ and hence no chord of $K$ passes through $X_\infty$. Instead, if $p \equiv 1 \pmod 3$, then $X_\infty$ lies on a chord of $K$. To show this, as $X^3 - Y^3 = (X - Y)(X - aY)(X - cY)$, we only need a pair $(x, y)$ satisfying either $x/y = a$ or $x/y = c$. The existence of such a pair comes from the following result due to Géza Kós:

THEOREM 2.3. *If $u_1$ and $u_2$ are the roots of the quadratic equation*

$$u^2 + u + 1 = 0 \tag{6}$$

*in* GF($p$), *then there exist integers* $x$, $y$ *with* $0 < x$, $y < \sqrt{p}$ *such that either* $xu_1 = y$ *or* $xu_2 = y$.

*Proof.* Let $r = \lfloor \sqrt{p} \rfloor$. First we prove that there exist $a$ and $b$ integers such that $0 < |a|, |b| \leq r$ and $au_1 = b$. We have $(r+1)^2 > p$ numbers in the form $\alpha u_1 + \beta$, where $0 \leq \alpha, \beta \leq r$, so there exist two of them, which are equivalent modulo $p$: $\alpha_1 u_1 + \beta_1 \equiv \alpha_2 u_1 + \beta_2 \pmod{p}$. Thus $a = \alpha_1 - \alpha_2$ and $b = \beta_1 - \beta_2$ can be chosen. The only problem is the sign of $a$ and $b$. One of them can be chosen to be positive, let this be $a$. If $b > 0$ then let $x = a$ and $y = b$, and we have finished the proof.

Therefore it can be supposed that $b < 0$. Let $c = au_2$. From (6) we get

$$u_1 + u_2 = -1 \quad \text{and} \quad u_1 u_2 = 1. \tag{7}$$

Thus $c = a(-1 - u_1) = -a - b$. As the signs of $a$ and $b$ are opposite and the absolute value of both is at most $r$, so $|c| \leq r$. If $c > 0$ then let $x = a$ and $y = c$, and we are done.

Therefore we may suppose that $c < 0$. Since $u_1$ and $u_2$ are negative, applying (7) gives

$$0 < -au_1 = a(1 + u_2) = a + c < a$$

and

$$0 < -au_2 = a(1 + u_1) = a + b < a;$$

therefore

$$(-au_1)(-au_2) = a^2 u_1 u_2 = a^2,$$

which is a contradiction, because $a^2 \leq p$. ∎

## 3. THE POINTS OF THE CUBIC CURVE

One can define an *abelian group* written additively on the non-singular points of a cubic curve with a rational inflexion so that

$$A, B, C \text{ are collinear iff } A + B + C = 0,$$

see [5]. The rational cubics yield the additive or multiplicative group of GF($q$) in this manner. With the terminology of abelian groups, arcs contained in cubic curves correspond to 3-independent subsets (see [7]).

DEFINITION 3.1. *Let $G$ be an abelian group. A subset $T \subset G$ is called 3-independent if*

$$t_1 + t_2 + t_3 \neq 0$$

*for any set $\{t_1, t_2, t_3\}$ of three distinct elements in $T$. A 3-independent subset is maximal if it is not contained in a larger 3-independent subset.*

EXAMPLE. Let $p$ be an odd prime and $k$ be the integer part of $p/3$. The set $T = \{0, 1, \ldots, k, k+1\}$ is a maximal 3-independent subset of the additive group modulo $p$ (see [7]).

The above maximal 3-independent subset together with Theorems 2.1 and 2.2 leads to the following

THEOREM 3.2. *For sufficiently large prime $p$, the set*

$$K^* = \{(x, x^3, 1) : x = 0, 1, \ldots, [p/3] + 1\} \cup \{(0, 1, 0)\}$$

*is a complete arc for $p \equiv 1 \pmod 3$, while $K^* \cup \{(1, 0, 0)\}$ is a complete arc for $p \not\equiv 1 \pmod 3$* (see [7]).

Our method explicitly gives a bound for $p$. From (5) for $c = 1/3$ we get $p > 1.7 \cdot 10^8$.

We now construct a class of maximal 3-independent subsets of the additive group modulo $p$.

CONSTRUCTION 3.3. *Let $k$ and $m$ be integers such that $k > 0$ and $(p+7)/(k+3) \leq m < (p+7)/(k+2)$. We construct the following set:*

*If $k$ is even, let*

$$T = \{0, \ldots, m-2\} \cup \{p - jm + 4 : j = 2, \ldots, k/2 + 1\}$$
$$\cup \{lm - 3 : l = 2, \ldots, k/2 + 1\}.$$

*If $k$ is odd, let*

$$T = \{0, \ldots, m-2\} \cup \{p - jm + 4 : j = 2, \ldots, (k+3)/2\}$$
$$\cup \{lm - 3 : l = 2, \ldots, (k+1)/2\}.$$

*We take numbers of the types of $p - jm + 4$ and $lm - 3$ alternately until $p - jm + 4 > lm - 3$ for all $j$ and $l$.*

THEOREM 3.4. *If $m > 5$ is not a divisor of $p + 9$ and $p + 12$, then $T$ is a 3-independent set of size $m - 1 + k$.*

*Proof.* Let $T_1$, $T_2$ and $T_3$ denote three subsets of $T$:

$T_1 = \{0, \dots, m-2\}$;

$T_2 = \{lm - 3 : l = 2, \dots, k/2 + 1 \text{ or } (k+1)/2\}$ depending on the parity of $k$;

$T_3 = \{p - jm + 4 : l = 2, \dots, k/2 + 1 \text{ or } (k+3)/2\}$ depending on the parity of $k$.

Let us take three distinct numbers $a_1$, $a_2$ and $a_3$ from $T_1 \cup T_2 \cup T_3$. We have to prove that $a_1 + a_2 + a_3 \neq 0$ modulo $p$.

1. $a_1, a_2, a_3 \in T_1$:

$a_1 + a_2 + a_3 \geq 0 + 1 + 2 = 3$,

$a_1 + a_2 + a_3 \leq m - 2 + m - 3 + m - 4 = 3m - 9 < 3 \cdot \dfrac{p+7}{1+2} - 9 <$ $p$, because $k \geq 1$.

2. $a_1, a_2 \in T_1$, $a_3 \in T_2$:

$a_1 + a_2 + a_3 \geq 0 + 1 + lm - 3 > 0$,

$a_1 + a_2 + a_3 \leq m - 2 + m - 3 + lm - 3 < 2m - 5 + p - 2m + 4 = p - 1$.

3. $a_1, a_2 \in T_1$, $a_3 \in T_3$:

$a_1 + a_2 + a_3 \geq 0 + 1 + p - jm + 4 > 0$,

$a_1 + a_2 + a_3 \leq m - 2 + m - 3 + p - 2m + 4 = p - 1$.

4. $a_1 \in T_1$, $a_2 \in T_2$, $a_3 \in T_3$:

$a_1 + a_2 + a_3 \geq 0 + 2m - 3 + p - jm + 4 > 0$,

$a_1 + a_2 + a_3 \leq m - 2 + lm - 3 + p - 2m + 4 \leq m - 2 + p - 2m + 4 + p - 2m + 4 = 2p - 3m + 6 < 2p$,

thus suppose that $a_1 + a_2 + a_3 = p$. From $a_1 + lm - 3 + p - jm + 4 = p$ we get $a_1 = (j - l)m - 1$. But $j - l$ is an integer and $0 \leq a_1 \leq m - 2$, which is a contradiction.

5. $a_1 \in T_1$, $a_2, a_3 \in T_2$: If there exist at least two numbers in $T_2$, then $k \geq 4$ and

$a_1 + a_2 + a_3 \geq 0 + 2m - 3 + 3m - 3 = 5m - 6 > 0$,

$a_1 + a_2 + a_3 \leq m - 2 + lm - 3 + (l-1)m - 3 = 2lm - 8 \leq (k+2)m - 8 < p + 7 - 8 = p - 1$.

6. $a_1 \in T_1$, $a_2, a_3 \in T_3$: If there exist at last two numbers in $T_3$, then $k \geq 3$ and

$a_1 + a_2 + a_3 \geq 0 + p - jm + 4 + p - (j-1)m + 4 = 2p - (2j-1)m + 8 > p$,

$a_1 + a_2 + a_3 \leq m - 2 + p - 2m + 4 + p - 3m + 4 = 2p - 4m + 6 < 2p$.

7. $a_1 \in T_2$, $a_2, a_3 \in T_3$:

$a_1 + a_2 + a_3 = lm - 3 + p - j_1 m + 4 + p - j_2 m + 4 = 2p + (l - j_1 - j_2)m + 5$. The sum cannot be $p$ or $3p$, only $2p$. Then $(l - j_1 - j_2)m = -5$. If $m > 5$, then $(l - j_1 - j_2)m$ can be 0 or $-m$ but not $-5$.

8. $a_1 \in T_3$, $a_2, a_3 \in T_2$:

$a_1 + a_2 + a_3 = p - jm + 4 + l_1 m - 3 + l_2 m - 3 = p + (l_1 + l_2 - j)$

$m-2$. Similarly, as in the previous case, this is never congruent to 0 modulo $p$ if $m>2$.

9. $a_1, a_2, a_3 \in T_2$:

$a_1+a_2+a_3 = p-j_1m+4+p-j_2m+4+p-j_3m+4 = 3p-(j_1+j_2+j_3)m+12$. This is non-zero modulo $p$ if $p+12$ is not divisible by $m$.

10. $a_1, a_2, a_3 \in T_3$:

$a_1+a_2+a_3 = l_1m-3+l_2m-3+l_3m-3 = (l_1+l_2+l_3)m-9$. This is non-zero modulo $p$ if $p+9$ is not divisible by $m$. ■

THEOREM 3.5. *$T$ is a maximal 3-independent set.*

*Proof.* To prove that $T$ is maximal, we find for all $t \notin T$ distinct elements $x_1, x_2$ of $T$ such that

$$x_1+x_2+t=0.$$

1. $m-1 \le t < 2m-3$:

Let $x_1 = p-2m+4$. Since $p-m+3 \le t+x_1 < p+1$, there exists $x_2 \in T_1$, for which $x_1+x_2+t=0$.

2. $(l-1)m-3 < t < lm-3$:

Let $x_1 = p-lm+4$. Since $p-m+1 < t+x_1 < p+1$ there exists $x_2 \in T_1$, for which $x_1+x_2+t=0$.

3. If $k$ is even, $j=k/2+1$ and $(k/2+1)m-3 < t < p-(k/2+1)m+4$:

Let $x_1 = (k/2+1)m-3$. Since $p+1-m = p+7-m-6 \le (k+2)m-6 = 2(k/2+1)m-6 < t+x_1 < p+1$ there exists $x_2 \in T_1$, for which $x_1+x_2+t=0$.

4. If $k$ is odd, $j=(k+3)/2$ and $(k+1)/2 \cdot m-3 < t < p-(k+3)/2 \cdot m+4$:

Let $x_1 = p-(k+3)/2 \cdot m+4$. Since $p+1-m < t+x_1 < 2p-(k+3)m+8 \le p+1$ there exists $x_2 \in T_1$, for which $x_1+x_2+t=0$.

5. $p-(j+1)m+4 < t < p-jm+4$:

Let $x_1 = jm-3$. Since $p-m+1 < t+x_1 < p+1$ there exists $x_2 \in T_1$, for which $x_1+x_2+t=0$.

6. $p-2m+4 < t \le p-m+2$:

Let $x_1 = m-2$. Since $p-m+2 < t+x_1 \le p$ there exists $x_2 \in T_1$, for which $x_1+x_2+t=0$.

7. $p-m+2 < t \le p$:

Let $x_1 = 0$. There exists $x_2 \in T_1$, for which $x_1+x_2+t=0$. ■

THEOREM 3.6. *Let $p$ be a prime, and let* $v = \dfrac{\sqrt{3 + (6\sqrt{p} + 9)\ln^2 p}}{\sqrt{p} - 1}$. *For any integer $s$ satisfying*

$$v + \frac{p+7}{v} - 4 < s \leq \left[\frac{p+7}{3}\right]$$

*there exists a maximal 3-independent set of cardinality $s$.*

*Proof.* The left side of the inequality comes from the bound (5).

There do not exist 3 numbers in $T_2$ and $T_3$ if $k \leq 6$. In this case we can omit the extra divisibility conditions of the previous theorem.

Otherwise let us suppose that $k \geq 7$. We can find $k$ and $m$ integers, such that $s = m + k - 1$, $(p+7)/(k+3) \leq m < (p+7)/(k+2)$ and $m$ is neither a divisor of $p+9$ nor of $p+12$. Let $k_0 = [(p+7)/s] - 2$ and $m_0 = s - k_0 + 1$. We have $m_0 < (p+7)/(k_0+2)$ and $s > (p+7)/(k_0+3)$. If $m_0 \geq (p+7)/(k_0+3)$, then we are done.

If $m_0 < (p+7)/(k_0+3)$, then let $k_1 = k_0 + 1$ and $m_1 = m_0 - 1$. We have $m_1 < m_0 < (p+7)/(k_0+3) = (p+7)/(k_1+2)$ and $m_1(k_1+3) = (s-k_0)(k_0+4) = s(k_0+3) + s - k_0^2 - 4k_0$. If $s - k_0^2 - 4k_0 > 0$, then this expression is greater than $p+7$, because of the magnitude of $s$ and $k_0$ coming from the theorem of Smith.

The pair $(m, k)$ ($(m_0, k_0)$ or $(m_1, k_1)$) satisfies $s = m + k - 1$ and $(p+7)/(k+3) \leq m < (p+7)/(k+2)$. If $m$ is neither a divisor of $p+9$ nor of $p+12$, then we have finished the proof. Otherwise let us suppose that $mu = p+9$ or $mu = p+12$. Now $(p+7)/(k+3) \leq (p+9)/u < (p+7)/(k+2)$ or $(p+7)/(k+3) \leq (p+12)/u < (p+7)/(k+2)$. The magnitude of $k$ implies that $u = k+3$. In this case either $m = (p+9)/(k+3)$ or $m = (p+12)/(k+3)$. Let $m^* = m - 1$ and $k^* = k - 1$. The magnitude of $k$ (which is greater than 2 but smaller than $C \cdot p^{1/4}$) implies that $s = m^* + k^* - 1$ and $(p+7)/(k^*+3) \leq m^* < (p+7)/(k^*+2)$.

In the following we will show that $m^*$ does not divide $p+9$ or $p+12$. Supposing the opposite, according to the previous calculations we have $m^*(k^*+3) = p+9$ or $p+12$. So both $m(k+3)$ and $(m-1)(k+4)$ are either $p+9$ or $p+12$. This is a contradiction, because the magnitudes of $m$ and $k$ implies that their difference $m - k - 4$ has absolute value greater than 3. ■

COROLLARY 3.7. *Let $p$ be a prime. For any integer $k$ satisfying*

$$[2.46 \cdot \ln p \cdot p^{3/4}] \leq k \leq \left[\frac{p+7}{3}\right] + 1,$$

*there exists a complete $k$-arc in* PG$(2, p)$.

## 4. APPLICATIONS

From Theorems 3.2 and 3.6, the set $K = \{(x, x^2, 1) : x = 1, \ldots, c \cdot p\}$ is an arc in PG(2, $p$) provided that $c$ satisfies certain conditions. The aim is to extend $K$ to a complete arc by adding as few points as possible. Two ideal points are enough if $1/3 < c < 1/2$ and $p$ is sufficiently large (see [7]). The question is how large $p$ should be. To prove that no affine point can be added, we consider a point $P(a, b, 1)$ $(a^2 \neq b)$. The collinearity of $P_1(x_1, x_1^2, 1)$, $P_2(x_2, x_2^2, 1)$, $x_1 \neq x_2$ and $P(a, b, 1)$ gives

$$a(x_1 + x_2) - x_1 x_2 - b = 0.$$

We estimate the number of solutions of the $f(X, Y) = a(X + Y) - XY - b = 0$. Simple computation shows that $f$ has a point for which $0 < X \neq Y < c \cdot p$, if

$$N(\mathscr{B}) \geq \frac{c^2 p^2}{p^2}(p + 1) - \frac{1}{p^2}(2\sqrt{p} + 4)p^2 \ln^2 p > 2.$$

This means that

$$c > \frac{\sqrt{2 + (2\sqrt{p} + 4)\ln^2 p}}{\sqrt{p} + 1}.$$

From $c = 1/3$ we get $p > 3 \cdot 10^7$. Note that the bound $p > 3 \cdot 10^7$ is sufficient for the constructions in [7], [8] and [9].

Faina constructed a cap from the plane arcs, described above. Thus the bound $p > 3 \cdot 10^7$ can also be applied for that cap. Finally I prove that no ideal points can be added to the cap constructed by Faina [3].

PROPOSITION 4.1. *Let $p > 3 \cdot 10^7$ be a prime, let $j$ be a fixed integer satisfying $p/3 < j < p/2$ and let $\alpha$ be a non-square element of* GF($p$). *Then the set defined by*

$$K = \{(x, y, x^2 - \alpha y^2, 1) \mid x = 0, 1, \ldots, j\} \cup \{(1, 0, 2j + 1, 0), (1, 0, -1, 0)\}$$

*is a complete cap of* PG(3, $p$).

*Proof.* Faina proved in [3] that only ideal points can be added to $K$. On the ideal line $x_2 = x_4 = 0$ we have two points of $K$, thus we take an ideal point $P(a, 1, b, 0)$ not lying on this line. For such a $P$ we want to find two points of $K$ such that these three points are on a common line. $P_1(x_1, y_1, x_1^2 - \alpha y_1^2, 1)$, $P_2(x_2, y_2, x_2^2 - \alpha y_2^2, 1)$, (where $y_1 \neq y_2$) and $P(a, 1, b, 0)$

are collinear if

$$x_2 - x_1 = a(y_2 - y_1) \quad \text{and} \quad b - a(x_1 + x_2) + \alpha(y_1 + y_2) = 0.$$

We can even fix $x_1$ and $x_2$ (they must be equal if $a = 0$) and find a solution of the arising linear system of equations for $y_1$ and $y_2$. If $a \neq 0$, then the solution is unique, and $p \neq 2$ implies $y_1 \neq y_2$. If $a = 0$, then there are many solutions, so we can find one where $y_1 \neq y_2$. ■

Note that the above bounds are unnecessary. Complete caps in the same range (without bounds on $p$) have been constructed by Faina and Pambianco, see [4].

## ACKNOWLEDGMENTS

I am very grateful to my supervisor, Tamás Szőnyi for his very valuable help, and I also thank Géza Kós for helping me in the question of adding the point (1, 0, 0).

## REFERENCES

1. U. Bartocci and B. Segre, Ovali ed altre curve nei piani di Galois di caratteristica due, *Acta Arith.* **18,** 423–449.
2. J. H. H. Chalk, The number of solutions of congruences in incomplete residue systems, *Canad. J. Math.* **15** (1963), 291–296.
3. G. Faina, Complete Caps having less than $(q^2 + 1)/2$ points in common with an elliptic quadric of PG(3, $q$), $q$ odd, *Rend. Mat. VII* **8** (1988), 277–281.
4. G. Faina and F. Pambianco, Una famiglia di $k$-calotte complete di PG(3, $q$), $q$ primo dispari, aventi $k - 2$ punti in comune con una quadrica ellittica, Rapp. tecnico No. 6-1994, Dip. Mat. Univ. Perugia. [English version to appear in *J. Geom.*]
5. W. Fulton: "Algebraic Curves," Benjamin, 1969.
6. R. A. Smith, The distribution of rational points on hypersurfaces defined over a finite field, *Mathematica* **17** (1970), 328–332.
7. T. Szőnyi, Arcs in cubic curves and 3-independent subsets of abelian groups, *in* "Colloquia Mathematica Societatis János Bolyai 52. Combinatorics, Eger" pp. 499–508, 1987.
8. T. Szőnyi, Note on the order of magnitude of $k$ for complete $k$-arcs in PG(2, $q$), *Discrete Math.* **66** (1987), 279–282.
9. T. Szőnyi, Small complete arcs in Galois planes, *Geom. Dedicata* **18** (1985), 161–172.
10. J. F. Voloch, On the completeness of certain plane arcs. *European J. Combin.* **8** (1987), 453–456.